পঞ্জীভুক্ত নম্বৰ - ৭৬৮ /৯৭ Registered No.-768/97

অসম ৰাজপত্ৰ

সত্যমেব জয়তে

THE ASSAM GAZETTE

অসাধাৰণ

EXTRAORDINARY

প্ৰাপ্ত কৰ্ত্তৃত্বৰ দ্বাৰা প্ৰকাশিত

PUBLISHED BY THE AUTHORITY

নং 651 দিশপুৰ, বুধবাৰ, 28 ছেপ্টেম্বৰ, 2022, 6 আহিন, 1944 (শক)

No. 651 Dispur, Wednesday, 28th September, 2022, 6th Asvina, 1944 (S. E.)

GOVERNMENT OF ASSAM

ORDERS BY THE GOVERNOR

INFORMATION TECHNOLOGY DEPARTMENT

NOTIFICATION

The 13th September, 2022

No. IT.38/2022/76.- The Governor of Assam is pleased to notify the "The Assam State Data Policy 2022" which will come into effect from the date of publication in the Official Gazette. The Government also reserves the right to make any amendment to the Policy from time to time as deemed fit and proper.

1. Preamble

1.1. Value potentials of data are widely recognized at all levels. Better use of reliable data can revolutionize the public sector, giving the means for efficient and transparent governance, more responsive service delivery, and innovation in sectors critical for societal transformation. With increased digitization and enhanced e-enabled engagements, the volume of data is also surging exponentially; however, the true potential of data in the government is yet to be realized fully. Even though large quantum of publicly funded data gets generated by various departments, organizations and institutions of the government, access to such data and digital systems remains confined to individual departments in a largely disconnected manner. Common guidelines on what data can be shared, how to make data available for use within and across departments, protocols for making data available for external parties etc. are usually not well delineated – impeding the emergence of a data-driven decision-making culturein government sector.

1.2. Recognizing the importance and potential value of data generated by the government departments, organizations, institutions and autonomous bodies for data-driven responsive governance, Government of Assam has pioneered data-driven governance for tackling pressing implementation challenges and achieving desired outcomes on high priority initiatives of the Government. Framing of the State Data Policy is one of the critical ingredients in this direction. The Assam State Data Policy seeks to define the rules of engagement with regards to all aspects of data management and governance, making optimal use of data for evidence-based decision making, and at the same time ensuring citizens' right to privacy which is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution.

1.3. The Assam State Data Policy provides the framework and guidelines for collection and collation of data, publishing of open data, and secure access to non-open data to catalyze theresearch and policy making by the departments, institutions and autonomous bodies of Assam Government; and sharing of data with bona fide external agencies collaborating with the government to strengthen policy processes and programme implementation.

2. Vision

The Assam State Data Policy envisions to intrinsically transform Government of Assam's ability towards harnessing cross-sectoral data generated with public resources to catalyze large scale social transformation by way of building digital and data capacity across the administrative hierarchy for improved and evidence-based policy process, better implementation and monitoring of development and welfare programmes, and efficient delivery of citizen centric basic services; and to encourage extensive use of data as value- asset for public good.

3. Objectives

The Assam State Data Policy (ASDP) is framed with the objective of laying down the principles and direction on data accessibility in both human readable and machine-readable forms while safeguarding citizens' right to privacy, towards enabling data-driven governance with data derivatives serving as public good to enhance government efficiency, improve access to quality public services and delivery of citizen centric benefits, and help advance digital transformation. This will also lay the foundation to build a Social Registry for efficient and targeted public service delivery. The ASDP shall promote data-usage as a value asset acrossdepartments, institutions, and autonomous bodies of Government of Assam, thereby contributing to the overall growth strategy for Assam.

4. Guiding Principles

4.1. Openness

Improving access to government-owned anonymized machine-readable datasets, enabling everyone to freely use, reuse and redistribute it. Openness provides the foundation for datasharing to unlock its value without compromising on its purpose and utility. For open data to flourish, a number of underlying policies and mechanisms, including technical frameworks for open access, need to be operationalized.

4.2. Privacy

Privacy is a fundamental right, flowing from the right to life and personal liberty under Article21 of the Constitution. Privacy of personal data and facts is an essential aspect of the right to privacy; and the Government as the custodian of information of citizens is responsible to safeguard it. Personal data shall be processed or shared only for specific, clear and lawful purpose and in a manner that preserves the privacy of citizens. The Personal Data Protection Bill, 2019[1] lays down a few key principles. ASDP is written with these principles in mind to ensure compliance seamless as and when the PDP law gets enacted.

4.3. Ethics and Equity

The State Data Policy shall ensure equity in the access of shareable data while conforming to highest level of ethical standards. There will be level-playing field that eliminates the barriers of data use, such as membership requirements, arbitrary decisions on allowing access to data, or unreasonable wait period for accessing the requested data; and at the same time ensuringprivacy of citizens' personal data.

---

1 The PDP Bill is yet to become a law but its parliamentary approval is expected rather soon.

4.4. Transparency

There will be transparent mechanisms for public access of open government data for public good with clear traceability to sources of data and information about any intermediate data transformations.

4.5. Legal Conformity

The State Data Policy will conform to all laws of the land including the laws enacted by the Parliament and State Legislature on privacy, data security and information protection. At the same time, there will be endeavors to mitigate / remove irrelevant legal barriers on the use ofdata by citizens and institutions for public good.

4.6. Protection of Intellectual Property

One of the key objectives of State Data Policy is to nurture innovation. It is therefore important to respect the intellectual property rights of the legitimate data creators / owners by restrictingaccess to IPR protected data. This would mean introducing checks and balances to ensure that data protected by IPRs is not hosted as Open Data. Concurrently, the policy would encourage / advocate increasing use of Creative Commons (CC) or similar public copyright licenses, enabling non-commercial uses of copyright protected data-sets to build upon the work of data creator / owner.

4.7. Interoperability and Standards

To enable discoverability and efficient use of existing data towards avoiding duplication and redundancies, the State Data Policy would pursue conscious efforts of removing the barriers to data interoperability, and establish techno-administrative protocols for more efficient data flow and usage between data systems, eluding the need for unreasonable amounts of time and energy on data access, cleansing and processing for reuse.

4.8. Data Quality and Usability

Poor data quality and lack of agreed standards are clear barriers to the effective use of data. The data that is being collected, processed and maintained by various entities, including government departments must be in meaningful and usable format; and is free from anomalies[2] which would inhibit further processing without significant investment on data cleaning and transformation. The policy defines guidelines to ensure that the shared data meets minimum quality requirements.

4.9. Data Security

With data now a critical part of modern life, interruption to data-driven services and activities can cause disruption to organizations , public services and businesses.

[2] Such as missing data, wrong attribute values, junk characters and the like.

Government therefore has a responsibility to ensure that data and its supporting infrastructure are safe, secure and resilient in the face of established, new and emerging cyber risks. This calls for a very high- level security during hosting and dissemination to prevent data manipulation and adversarial attacks or misuse or unauthorized access to data. The provisions under the State Cyber Security Policy 2020 should be adhered to in implementing the systems and applications related to data collection, collation, processing, and storage.

4.10. Accountability and Formal Responsibility

The State Data Policy provides for guidelines that ensure accountability and responsibility with respect to the sharing of open data, as well as the adherence of rules relating to access ofnon-open data.

4.11. Sustainability

The goal of sustainability is to ensure that open data sharing is not hindered due to external factors. This implies sustainability on all fronts that include technical, economic, financial, legaland other relevant criteria.

5. Definitions

5.1. **Data:** Representation of information, numerical compilations and observations, documents, facts, maps, images, charts, tables, reports and figures,concepts in digital and/or analog form.It covers all aspects of government functioning including G2G, G2B, G2C.

5.2. **Data-set:** Collection of logically related features, attributes or variables including processed dataor information.

5.3. **Data Archive:** The digital location where machine-readable data is stored, worked upon / analyzed, documented prior to a cut-off past date.

5.4. **Data Generation:** Initial collection of data or subsequent addition of data to the same specification. This may be data specifically collected for a particular objective or may be a consequence of the authorized administrative processes of the Government.

5.5. **Data Principal:** A natural person who is subject of the handled data by which that person can be identified.

5.6. **Data Fiduciary/Custodian:** Any person, including the State, a company, any juristic entity orany individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

5.7. **Data Processor:** Any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a Data Fiduciary.

5.8. **Metadata:** *Data about data*. The information that describes the data source and the time, place, and conditions under which the data were generated. Metadata informs the user of who,when, what, where, why, and how data were generated. Metadata allows the

data to be traced to a known origin and known quality. Metadata consists also of structural aspects such as defining the data and datasets, administrative aspects, such as the processing and audit trail information, descriptive aspects, such as time series and statistical data features (i.e. data source, and the time, place, and conditions under which the data was created)as well as the methods, procedures, concepts, variables, classification, and nomenclature used, including publication date and data coverage.

5.9. **Data Standards:** Frameworks that define and embed data handling functions (e.g. data collection, management, transfer, integration, publication); and operate on data in a manner that complies with data format and data syntax specifications produced and maintained by standards bodies.

5.10. **Information:** Data embellished with a context, in other words, "Processed data."

5.11. **Personally Identifiable Information:** Data about or relating to a Data Principal who is directly or indirectly identifiable, whether online or offline, or any combination of such features with any other information; and shall include any inference drawn from such data for the purpose of profiling.

5.12. **Sensitive personal data:** Such personal information which consists of information about Data Principal relating to Password, Biometric information, Official identifier, Financial Data, Information received by body corporate for processing lawful contract or otherwise, Health Data, Genetic Data, Transgender /Intersex status, Health Data, Genetic Data, Transgender /Intersex status, Sexual Orientation and Sex life et. al.

5.13. **Anonymization:** In relation to personal data, refers to the irreversible processes of transforming or converting personal data to a form through which a Data Principal cannot be identified even if the information is combined with other information, after reasonably considering factors such as time, cost and technology.

5.14. **Aggregation:** Refers to the process of creating higher level data by combining data across DataPrincipals so that it does not reveal any personally identifying information about a Data Principals. Aggregation is a way of anonymizing data.

5.15. **De-identification or pseudo anonymization:** Means the process by which identifiers from personal data may be removed, or masked, or replaced with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the Data Principal.

6. Scope and Applicability

6.1. The Assam State Data Policy provides the framework and guidelines for collection, collation and processing of data in machine readable format; classification and publishing of open data; secure and restricted access of non-open data across departments towards effective policy formulation and programme implementation; and secure permissioned access of anonymized /de-identified datasets to entities outside of government for bona fide research and analytical studies aimed at policy design and implementation.

6.2. The Assam State Data Policy shall be applicable to all data and information created,

generated, collected, and archived by departments, institutions, organizations, autonomous bodies of Government of Assam, using public funds provided by the State or the Central Government. All such data shall be stored and maintained in the National / State Data Centre (NDC / SDC) of Government of Assam preferably on security control-based cloud hosted technical architecture or in MeitY empanelled Cloud service providers, with appropriate data management and data security protocols; and with systems and procedures in place for access and use by all stakeholders in the State as defined under this policy. This Policy will also apply to data that is recurring in nature and generated owing to automation of governmentprocesses and the results emerging out of these for delivery of services and benefits to citizens and businesses, as well as the legacy government data that is still available in non-machine - readable form within the State of Assam. Government of Assam will proactively engage with Bodoland Territorial Council, Karbi Anglong Autonomous Council and North Cachar Hills Autonomous Council for adoption of Assam State Data Policy within their territorial jurisdiction.

7. Data Classification

All departments, institutions, public sector undertakings and autonomous bodies functioningunder Government of Assam, shall classify all data generated by them to the following data access structure:

7.1. **Open Access Data**: A dataset, including geospatial data, is classified to be open if anyone is free to use, reuse, and republish for lawful purposes, without restrictions from copyright, patents or other mechanisms of control. Access to open data generated from public funding shall preferably be accessible in machine-readable formats that are optimized for machine processing for easy use without any process of registration/ authorization. Sensitive personaldata shall never be classified as Open Access data.

7.2. **Permissioned Access Data:**

a. The datasets which can only be accessed by others only with prior permission from the government or the data owner including body corporate through defined procedures and in accordance with associated terms of use. Personal identifiers of raw data or a database dump must be masked before sharing with academic / research entities, civil society organizations or others, predominantly for public good oriented research and analytical works. The datasets classified as Permissioned Access Data shall contain lowimpact data, so that the loss of confidentiality or integrity[3] do have none or limited adverse effect on the concerned individuals, organization and the government department who owns the information. Rules of anonymization[4], aggregation[5] or de-identification[6] shall invariably beenforced before classifying a dataset as Permissioned Access Data.

---

[3] A loss of confidentiality is the unauthorized disclosure of information. A loss of integrity is the unauthorized modification or destruction of information.

[4] The irreversible process of transforming personal data to a form through which a data subject cannot be identified even if the information is combined with other information.

[5] Refers to the process of creating higher level data by combining data across data subjects so that it does not reveal any personally identifying information about a data subject. It is one of the easier ways of anonymizing data.

[6] De-identification or pseudo anonymization means the process by which identifiers from personal data may be removed, or masked, or replaced with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data subject.

b. Any department / organization of Government of Assam may share Permissioned Access Datasets with other government departments / organizations; however, the recipient departments / organizations must seek approval from the data owners for any onward sharing of data with Third parties, which inter-alia might also include another department / organization. Any such sharing (or onward sharing) of data amongst departments/ organizations must be subject to the restrictions of applicable laws and rules[7], as well as waivers provided by the Center for Data Management (CDM), which will be established for implementation and ensuring compliance of the Assam State Data Policy. The data sharing department / organization of the government shall be solely responsible for adherence of theselaws and rules.

7.3. **Non-shareable data**: Sensitive personal data[8] and the datasets which are confidential in nature[9] and are in the interest of the country's security in not opening to the public would fall in the negative list. This includes data/information that is expressly prohibited from disclosure as per exemptions defined under sections 8 and 9 of the Right to Information Act, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the Collection of Statistics Act, 2008 and rules framed thereof. Additionally, when the Personal Data Protection Act gets enacted, its provisions must be adhered to in deciding the shareability on any specific dataset.

8. Data Management and Governance Framework

A streamlined data governance framework has been laid down towards functioning and enforcement of the Assam State Data Policy for effective policymaking, efficient delivery of quality services and benefits to citizens; and to help extract value from all the data held in thestate. The following framework shall be adopted across all government departments and public funded organizations in Assam.

8.1. Data Collection and Ownership

a. Collection of primary data shall predominantly be the responsibility of government departments and institutions mandated for policy process, programmatic implementation and/or service delivery. Data collection, irrespective of the primary data acquisition mechanisms[10], shall be ethical and compliant with prevailing data privacy

---

[7] Explanatory example: It is assumed that Assam State AIDS Control Society (ASACS) receives request from another department of the government for sharing individual level data (without personal identifier) of NACP beneficiaries for the purpose of designing a new welfare scheme for all PLHIV (People Living with HIV/AIDS) population of the State. The affirmative response of ASACS will be contingent upon the adherence of NACO Data Sharing Guidelines 2018 and the procedural requirements stipulated thereon. ASACS as the data sharing organization shall be solely responsible for adherence of these NACO guidelines; and shall insists on the data protection and usage rules by the recipient department by way of formal undertakings. If the recipient department intends forward the ASACS shared data to another department or to a research organization, it must obtain explicit approval from ASACS before it could so.

[8] Such as Aadhaar or any Unique ID Data, biometric data, medical records including genetic data, Information received, stored or processed by body corporate for under lawful contract etc.

[9] High impact data wherein the loss of confidentiality or availability in public domain could have severe adverse effect on the individuals and/or the government department who owns that information.

[10] These could be by way of either electronic / paper-based data acquisition by human intermediaries or non-human collection via bots, drones, aerial imaging, satellite and other emerging IoT (Internet of Things) devices.

and security legislations and rules thereof. The ownership of data shall reside with the Data Principals with fair use rights of department / institution / autonomous bodies for which the data has primarily been generated, while the Center for Data Management would serve as the custodian of all these publicly funded digital data systems.

b. Only the Data Fiduciary, either on its own or in conjunction with others, shall determine the purpose and means of collecting and processing of personal data, which shall be collected only to the extent that is necessary for the fulfilment of designated purposes. At the time of collecting personal data, the Data Fiduciary shall notify the Data Principal in concise and easilycomprehensible language:

   (i) the nature and categories of personal data being collected and the purposes for which;

   (ii) the data is to be used / processed;

   (iii) the period for which the personal data shall be retained; individuals or entities including other data fiduciaries or data processors with whomher/his personal data may be shared;

   (iv) the right of the data principal to withdraw her/his consent and the procedure for suchwithdrawal;

   (v) procedure for grievance redressal.

c. Primary data collection shall be conducted with the utmost integrity to ensure that the collected/ processed data is free of error and bias. Input constraints, automatic data consistency checks and string validation rules shall be used to minimize data quality challenges at the entry stage.Wherever feasible, the collection of primary data should be through electronic means; relevant investments shall be made for transitioning to electronic data collection platforms from paper- based systems. In scenarios where paper-based data collection is unavoidable, the collectedraw dataset will be digitized by the corresponding department within one month of itscollection. Automated processes, algorithms and other state-of-the-art data cleaning mechanisms shall be applied to the extent possible for validating collected data for consistency and quality. Robust security measures such as encryptions, firewalls, and access controls shall be established for data storage to prevent unauthorized access, manipulation and loss of non-shareable data.

8.2. Lawfulness of Processing

a. No personal data shall be processed except for clear, specific and lawful purpose. The collection and processing of personal data shall be lawful only if one of the following applies:

   (i) Data Principal has given explicit consent to process her/his personal data for certain defined purposes[11];

---

[11] If the Data Principal's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this policy shall not be considered lawful.

(ii) Processing is necessary for compliance with a legal obligation, or delivery of public service / benefit and eliciting beneficiary feedback on scheme delivery, or the performance of acontract to which the Data Principal is party.

(iii) Processing is necessary in order to protect the vital interests of the Data Principal oranother natural person(s).

b. For the purpose of social protection benefits or online services directed at children below theage of 18 years, the processing of personal data of a child shall be lawful only if and to the extent that consent is given by her / his parent or legal guardian. Every person[12] processing personal data shall do so in a fair and reasonable manner and ensure the privacy of the Data Principal.

8.3. Processing of special categories personal data

Processing of personal data that reveals caste, ethnic origin, race, religious beliefs; genetic and biometric data for the purpose of uniquely identifying a natural person; data concerning health and sexual orientation of a natural person shall be prohibited. These restrictions could however be waived off if the Data Principal gives explicit consent to the processing of these personal data for one or more specified purposes; or the Data Principal is physically or legally incapable of giving consent.

8.4. Data Interoperability

a. Data interoperability will be achieved by way of (1) standardizing data elements that appear across datasets, and (2) making data available through an open and machine-readable format[13], together with their metadata at best level of precision and granularity to help establish common understanding of the meaning or semantics of the data, ensuring correct and proper use and interpretation by its owners and other related users.

b. Data Fiduciaries shall be required to prepare comprehensive and mandatory Meta Data Catalogue[14], including the data owners and source of truth and its periodic updates from timeto time; and publish these to improve awareness of what data exists and whether and how datasets across geographies/sectors/federal levels/time periods can be integrated and/or cross-referenced.

---

[11] If the Data Principal's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this policy shall not be considered lawful.

[12] In this context, the person could be an individual, a Hindu undivided family, a firm or company, an association of persons or a body of individuals, any other juristic entity, and the State.

[13] Based on the analysis of current data formats prevalent in the government, the publishing data could be made available in any appropriate formats, such as ODT/ODS, CSV, XLS, XML, RDF, GML; and for fast changing datasets RSS/ATOM syndication format.

[14] Metadata catalogue contains definitions, datatypes, length, encoding scheme and all other attributes of a typical data element like name, address, income etc., which could be stored in multiple ways in multiple applications.

8.5. Creation of a Social Registry

a. Data Interoperability standards will lay the foundation for creating a Social Registry as an integrated data system that support outreach, intake, registration, and determination of potential eligibility for one or more social programs. It will provide a "gateway" for people (individuals, families) to register and be considered for potential inclusion in one or more social programs based on assessment of their needs and conditions. It will contain information on all registrants, whether or not they are deemed eligible for, or enrolled in, select social programs. It will make use of a variety of system elements, namely:

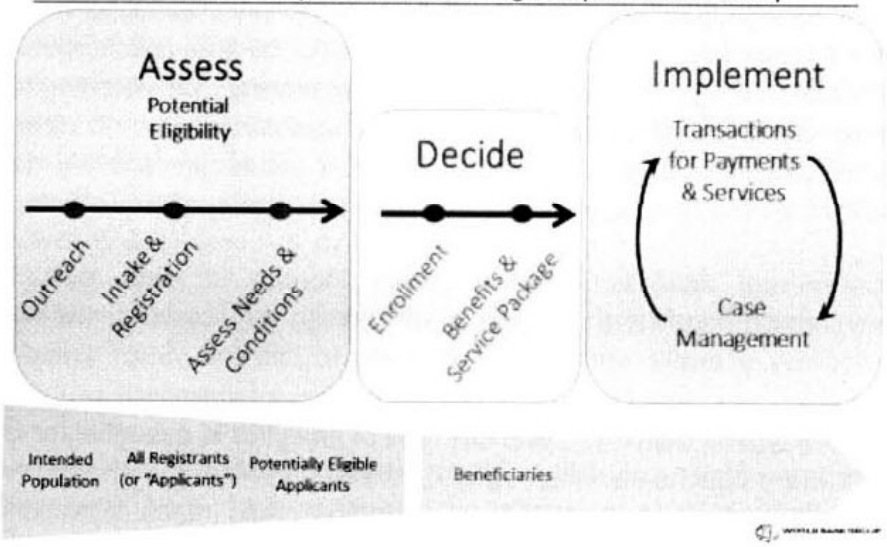
(i) data and information;

(ii) software;

(iii) database management; and

(iv) ICT infrastructure, as well as institutional aspects (people, procedures, documentation, etc.)

Figure 1 – Social Registries Support Determination of Potential Eligibility within the Delivery Chain for Social Programs (blue shaded areas)



b. The State DBT Cell of the Finance Department shall be vested with the responsibility of building and operationalizing an integrated Social Registry through a Digital Infrastructure for DBT Schemes (DIDS) platform, subject to the overall supervision of Stata Data Management Steering Committee (SDMSC). The State DBT Cell will also issue the Operational Guidelineswith the approval of the SDMSC.

8.6. Securing the Data System

High level security on the storage and dissemination of data is a mandatory

precondition to prevent adversarial and manipulative attacks, as well as unauthorized access and misuse of restricted / confidential datasets. Technical audit of data systems security will have to be conducted by CERT-In[15] empaneled information security organizations to diligently assess potential threats, risks and vulnerabilities; confirm that the information resources and data assets are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorized access to the data system. In case vulnerabilities are identified, the Security Auditor would recommend relevant remedial actions to ensure compliance of established information security norms and guidelines. In addition, the Centre for Data Management will issue from time to time the administrative (non-technical) measures and procedures for securing data assets; and periodically review their compliance across all departments and institutions.

8.7. Rules of Access to non-open Data

a. Access of non-open government data, especially the permissioned access datasets to entitiesoutside of government, shall be governed by the rules and criteria delineated by the Center for Data Management. Guiding questions such as whether data is anonymized / de-identified, aggregated, users of the shared datasets and purpose of use, levels of sensitivity of personal data etc. would be the critical determinants in making the data-sharing decisions. Further, alldata sharing / provisioning shall be only through secured high quality, reliable and easy to use APIs[16] with no direct access to primary databases; and government departments / institutions sharing data shall be responsible for the correctness, completeness and authenticity of shareddata.

b. Cross departmental analysis, which involves looking at data sets in different departments through identifiers[17], is key to enhancing public sector performance and improving delivery of public service and benefits to citizens. Such cross-department analysis can often give new insights for targeted policy interventions or even identifying gaps in service / benefit delivery[18]; and this type of analytics is essential for Government of Assam to better target its developmentand efforts. Likewise, the sharing of non-Open Data for bona fide research and analytical studies could result in actionable policy advice and programmatic guidance to government, and should be encouraged.

---

[15] Indian Computer Emergency Response Team (https://cert-in.org.in/).

[16] Application Programming Interfaces.

[17] Such as demographic information, phone number, ration card, EPIC, Aadhaar – to name a few.

[18] E.g. Orunodoi beneficiary household with family member as serving employee of cooperative societies.

c. Permissioned access of data for research and analytical studies will require requisite due diligence, establish a genuineness of the research for a public non-commercial purpose, andwhether the research / analytical study outputs meet the yardstick of public good. Formal data sharing agreements with the concerned institutions / think-tanks / universities shall be executed articulating the purpose and mode of sharing data; conditions for data sharing and terms of use; mechanisms of compliance due diligence; provision for penalties for any violations of the terms of use; data security safeguards to be applied by the recipient institution / university; and defined period of data retention by the recipient(s). No permissioned access data shall be permanently retained for any purpose beyond the time permitted, nor can be shared with any other third party, nor can the data be used for any commercial purpose.

8.8. Redressing Grievances of Data Principals

The Center for Data Management (CDM) shall ensure operationalization of effective and efficient mechanisms to redress the grievances of Data Principals. There shall be easy and well publicized procedures to make complaints to the Data Fiduciary with regard the contravention of any of the provisions of ASDP or the rules made there under, which has caused or is likely to cause harm to the concerned Data Principal. Such complaints /grievances shall be resolved by the Data Fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint. Government of Assam shall notify a detailed appeal process and an empowered Appellate Authority for the Data Principal to escalate her/his data related complaint if the grievance is not resolved by the Data Fiduciary within the specified period; or has been rejected; or Data Principal is not satisfied with the manner in which the grievance is resolved. The Appellate Authority will follow an appropriate quasi-judicial process to decide on the escalated grievance of the Data Principal; and the Center for Data Management shall function as the Secretariat/Registry of the empowered Appellate Authority.

9. Implementation and Administrative Framework

9.1. Center for Data Management

a. Government of Assam, through gazette notification, shall establish Center for Data Management under the administrative control of IT Department for the purpose of facilitating and enforcing implementation; and to ensure compliance of the provisions of Assam State Data Policy. The CDM shall be empowered to formulate rules needed to ensure adequate implementation of the State Data Policy; issue notifications, operational clarifications, guidelines and advisories, and code of practices for nuanced interpretations of the Policy and to promote good practices; and recommend amendments to the Policy for Cabinet Approval, as and when such unavoidable need arises.

b. Towards realization of the vision and objectives of Assam State Data Policy, and to protect the interests of Data Principals, the Center for Data Management (CDM) shall have the mandate to:

(i) Make sure that information is appropriately accessible within a protected and

trusted environment subject to access, security, and privacy rules; and periodically review data policy compliance by departments, institutions, organizations and autonomous bodies covered under the State Data Policy.

(ii) Accord approvals on

1. publishing and usage of restricted access data, with appropriate privacy safeguards, for important and high-level initiatives of Government of Assam; and

2. exceptions not envisioned in the ASDP on data collection, processing, storage,publishing, usage, and adherence to data standards.

(iii) Prevent misuse of personal data and take prompt and appropriate action in response to personal data breach.

(iv) Review Data Privacy measures from time to time and take action to improve/refine the legal, technical and administrative framework and processes for ensuring better data privacy.

(v) Monitor technological developments and practices so that the provisions of ASDP could be adapted in tune with technological advancements and emerging digitalization practices for socio-economic empowerment of the State and its people.

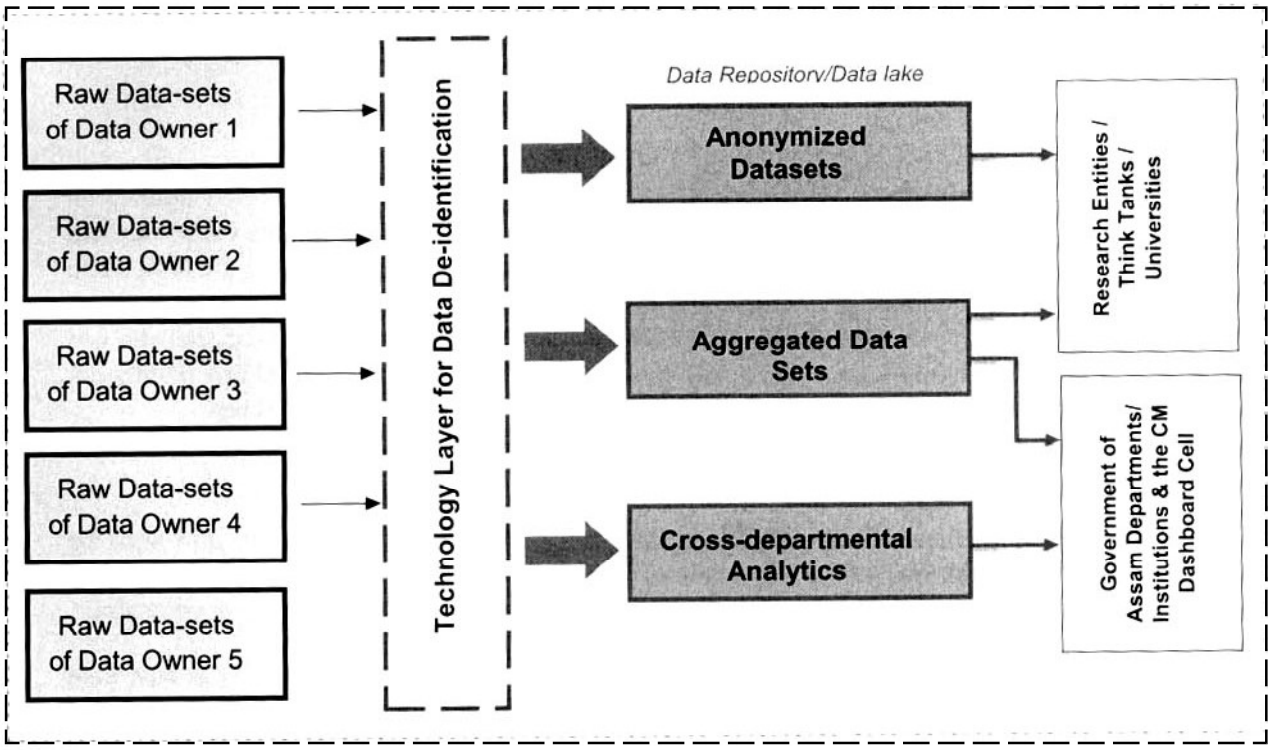
(vi) Undertake measures for promotion of research and innovation on emerging technologies,data driven governance, and other related public interest areas.

(vii) Receive, inquire and resolve the grievances of data principal and related stakeholders with regard the contravention of any of the provisions of ASDP or the rules made there under.

(viii) Initiate appellate action on any grievances against the decision of the Data-Inter- Departmental Committee (DIDC).

(ix) Perform other related functions as may be prescribed by government from time to time.

c. The Center for Data Management shall proactively put in place a technology layer for ensuring anonymization, aggregation and creation of cross departmental analytics that cater to both government entities as well as research agencies / think-tanks / universities; and shall establish a state-of-the-art data repository / data-lake of government data as envisaged below:



d. The Center for Data Management will be a lean professional organization and will be established as Government of Assam society under the Chairmanship of the Chief Secretary.The Chief Data Officer (CDO), appointed by the government, shall be the *ex-officio* Chief Executive Officer of the CDM with appropriate administrative and financial authority, as well as budgetary provisions for taking all operational level decisions emanating from Assam StateData Policy. The CDO shall exercise all powers and do all such tasks which may be exercisedor done by the Data Inter-Departmental Committee (DIDC); and shall be assisted by a professional team[19] having qualification, specialized knowledge, and experience in the field ofdata management, data science, data security, digital technologies and systems engineering,cyber and privacy protection laws, public administration or related subjects. The CDO may appoint consultants and solicit services of relevant experts considered necessary for the effective discharge of CDM mandates.

e. The Executive Committee of Center for Data Management Society shall function as the Stata Data Management Steering Committee (SDMSC) to coordinate and monitor the implementation of State Data Policy through close collaboration with all state government departments and agencies. SDMSC will include Senior-most Secretaries of IT, Finance, Revenue, ARTPPG, P&RD, Urban Development, Health, Education Departments, and Forests dealing with large datasets. SDMSC shall also function as Apex deciding authority on all issues relating to Data Governance standards and benchmarks in the State.

---

[19] Professional team assisting CDO will be comprised of Data Science Specialist, Technical Systems Architect and Data Policy Compliance Counsel.

f. The Center for Data Management (CDM) shall be the nodal empowered agency for coordinating with the Data Protection Authority of India, proposed in the Personal Data Protection Bill and relevant Central Government entities; and specifying the Meta Data Catalogue standard and associated activities in alignment of the proposed National Data Governance Framework. The CDM will also draw inputs from the guidelines and standards issued from time to time by the India Data Management Office (IDMO) for developing rules, standards, and guidelines under Assam State Data Policy.

9.2. Chief Data Officer (CDO)

a. The Chief Data Officer shall be appointed by Government of Assam, and shall be responsible for day-to-day implementation of the State Data Policy, as well as for data management and governance, and effective utilization of data across the government:

b. Lead all the data initiatives of the Government of Assam; and own the critical data quality and data sharing efforts such as developing Meta-Data Catalogue and Standards.

c. Lead on cross-department analytics initiatives for enhanced performance by departments and improved delivery of public service and benefits to citizens; and help departments in minimizing inclusion and exclusion errors in schemes.

d. Chair the DIDC which is responsible for taking decisions on all aspects of data-governance, and to help collect, collate, process and publish data in line with ASDP.

e. Define appropriate process for the identifying and releasing open access datasets. Proactively release as many datasets as possible under Open Access Data classification.

f. Ensure data privacy of the Data Principals and citizens while sharing data with all appropriate and possible safeguards.

g. Recommend to the Chairperson of CDM for approval on the department specific Negative List of confidential datasets prepared by DIDC in consultation with respective departments/institutions/autonomous bodies.

h. Work with the Data Principals and Processors to help transform departmental data into actionable insights for targeted policy interventions or even identifying gaps in service / benefit delivery.

9.3. Departmental Data Officers and Sub-Data Officers

a. Departments/Institutions/Autonomous Bodies under Government of Assam would nominate a Data Officer with reasonable seniority and experience on digital data management / governance. The Departmental Data Officer shall be responsible for anchoring the efforts of organizing and storage of department's data in machine-readable open format, deciding on open data classifications, compliance to the State Data Policy, and carrying out the decisions of the Data Inter-Departmental Committee (DIDC) on all aspects of data-use and data governance.

b. The Sub-Data Officers would be responsible for identifying open access datasets

pertaining to their department in the State Data Repository along with their metadata to facilitate easy sharing, collaboration and interoperability. All Sub-Data Officers shall report to the Departmental Data Officer for works relating to Assam State Data Policy; and be responsible for ensuring quality and correctness of datasets of his/her unit/division.

9.4. Data Inter-Departmental Committee (DIDC)

a. Data Inter-Departmental Committee (DIDC) shall be constituted with all the Departmental DataOfficers, under the Chairmanship of the Chief Data Officer; and shall be responsible for taking decisions on all aspects of data-governance, and to helps collect, collate, process and publishdata in line with ASDP.

b. The DIDC shall function in the following 5 streams:

(i) Open Data Stream

1. Identify datasets that can be classified as Open Access Data; and undertake anonymization / de-identification exercise to ensure legitimate and legal use of such datasets, so that the shared open data may not be combined with other datasets to extract Personally Identifiable Information (PII).

2. Develop and publish Meta-data Catalogues, Standards and Resources for Open Access Data.

3. Prepare Negative List of Datasets that cannot be shared due to legal restrictions or policy decisions.

(ii) Data Quality Stream

1. Develop and institutionalize the Meta-Data Catalogue as an ongoing initiative.

2. Work on data quality and refinement by various survey and data validation methods.

3. In consultation with line departments identify schemes / mechanisms through whichinclusion, exclusion errors can be minimized.

(iii) Analytics and Evidence based Decision Making Stream

1. Develop the problem definitions that could be addressed by inter or cross-departmentanalytics.

2. Define the required data and program to manage those initiatives by institutionalizingdata sourcing, quality, reporting and analytics.

3. Develop the analytic layer for reporting and visualizations.

(iv) Compliance and Governance Stream

1. Conduct a periodic ASDP compliance audit including the adherence to data standards and other guidelines issued from time to time. Report the compliance audit report and recommendations to the Center for Data Management (CDM).

2. Act on issues and complaints from user departments, and also data-oriented discrepancies that impede citizens availing specific public services and/or social welfare benefits.

(v) Managing partnerships and Data Sharing Stream

1. Be the nodal entity to manage partnerships with external stakeholders such as research organizations / think-tanks / universities etc.

2. Evaluate the proposals for data access for both 'public good' and allow access as prescribed in the State Data Policy.

3. Obtain the consent and necessary data protection undertakings/agreements from all permissioned access data users for the intended use per their proposal.

c. The Data Inter-Departmental Committee (DIDC) shall be assisted by professionals conversant in data analysis, portal development, database development, visualization, analytics, programming, and other such professionals as required for the implementation of the policy.

9.5. Training and Skill Development

Alongside a strong IT infrastructure, governance framework and guidelines for data governance, it is crucial that the government manpower is regularly upskilled on technical skills, practices and know-how of data handling, management and use such that the State Data Policy may be successfully implemented, and data gets effectively used for evidence- based decision making. Training and skill development shall be designed to equip all government manpower with the appropriate and up-to-date knowledge and skill sets such that a culture of data-driven governance is encouraged and adopted by all in Government of Assam. DIDC, in consultation with the Center for Data Management (CDM) and ART-PPG Department, shall lay down a plan for regular training and skill development of all government manpower, especially the manpower involved in data collection, processing, management and/or use.

9.6. Budgetary Provisions

a. The implantation of Assam State Data Policy shall entail requirement of capital and operating resources for departmental data owners to transform analog datasets to machine-readable digital data and for conversion of existing digital data into open interoperable formats, towards enabling efficient data usage across the government with all appropriate data sharing safeguards. Resources will also be necessary for the CDM to carry out its mandate, such as helping architect / upgrade departmental data systems, conducting data quality appraisal and refinement, designing big-data storage solutions, and creating state data repository / data lake, training and capacity building,

and technical assistance to SDMSC on issues relating to data governance standards and data management bench-marks; as well as on the operational expenses and DIDC functioning. Additionally, there will be need for considerable capital investments by DITEC in upgrading IT and cloud infrastructure in the State Data Centre (SDC) to meet the enhanced departmental demands for data-storage and network computing capabilities. Budgetary requirements for all these tasks will have to be detailed out – for the CDM, DITEC, and at the levels of each department / institution / organization / autonomous bodies of Government of Assam for transforming Assam State Data Policy vision into a reality.

b. Separate head-of-account in department specific budgets shall be created to provision earmarked resources for creating and/or improving departmental data systems. These shall exclusively be for the software systems and manpower involved in data system strengthening; and no budgetary allocation/expenditure shall be made towards procuring and installing server-side hardware infrastructure at departments, which invariably causes fragmentation and duplication of publicly funded data assets. The capability enhancement of SDC and cloud infrastructure, for the purpose of ASDP implementation, shall exclusively be within the realms of IT Department / DITEC mandate; and shall be designed and implemented in consultation with the CDO and DIDC.

9.7. Policy Implementation Support and Compliance Monitoring

a. Detailed Operational Guidelines for ASDP implementation will be published by the CDM with approval of SDMSC; and will be updated on an annual basis to factor in the rapid innovations in data governance and data management practices. The Operational Guideline shall include the technology and standards data collection, processing, storage and sharing; criteria and mechanism for restricted access data sharing; suggested format for publishing Metadata catalogues; model data sharing and licensing frameworks. The CDM will also organize training and handholding support for Departmental Data Officers to effectively deliver on their mandated responsibilities; and shall also monitor compliance of policy norms and guidelines, routine adherence to the practice of encryption, anonymization and/or deidentification personal data, as well as on the five streams of DIDC's functional mandate.

b. The Data Policy Compliance Specialist of the Center for Data Management shall have the obligation of conducting the policy compliance monitoring every six months; and the year-end compliance monitoring exercise will also involve an independent Data Protection Impact Assessment (DPIA) to identify risks arising out of the collection and processing of personal data, and to minimize these risks as far and as early as possible. The six-monthly report on ASDP compliance will be submitted to the SDMSC for considered review and necessary guidance. The SDMSC will in turn furnish an annual policy compliance report to the Cabinet.

10. Benefits of State Data Policy

10.1. **Equity of data-access**: The ASDP practice of open access data will ensure better access toall bona fide users.

10.2. **Maximizing data use**: Access to government-owned data will enable the more extensive use of the information to deliver services and facilities in an efficient and transparent manner.

10.3. **Maximized integration**: Adoption of common standards and best practices across various datasets and MIS would facilitate the integration of individual datasets.

10.4. **Interoperability to avoid duplication**: By facilitating the sharing of required data across departments, the need for separate bodies to collect the same data will be minimized. This will result in significant time and cost-saving in data collection, and also eliciting a rounded perspective on the performance of government initiatives and schemes.

10.5. **Better decision making**: Availability of data will enable data-driven decision making along with avenues and platforms for monitoring, reporting and planning.

10.6. **Better tracking for policy implementation**: Real-time availability of data will allow and openpathways for live tracking of policy implementation and impact, especially for welfare schemes.

10.7. **Enhanced and efficient delivery of services**: Data sharing and interoperability through thispolicy will be instrumental in reducing leakages and plugging loopholes in the delivery of welfare services.

11. Period of Validity of State Data Policy

The Assam State Data Policy in its present form will remain valid till any further revision that incorporates transformative global innovations in data governance and data management practices.

ANURAG GOEL,
Principal Secretary to the Government of Assam,
Information Technology Department.

Guwahati : Printed and Published by the Director, Directorate of Printing & Stationery, Assam, Guwahati-21.
Extraordinary Gazette No. 1301 - 10 + 10 - 28 - 09 - 2022. (visit at– dpns.assam.gov.in)